STATEMENT OF RELEVANCE

>
>
> MULTI-PLACE TICKET ISSUE USING SMART CARD
> Pub. No.: 20-00057210 [JP 2000057210 A]
> Published: February 25, 2000 (20000225)
> Inventor: GOLDSTEIN THEODORE CHARLES, ZIEGLER JONATHAN B
> Applicant: SUN MICROSYST INC
> Application No.: 11-180905 [JP 99180905]
> Filed: June 25, 1999 (19990625)
> Priority: 106600 [US 106600], US (United States of America),
> June 29, 1998 (19980629)
> INTL CLASS: G06F-017/60; G09C-001/00
> ABSTRACT
> PROBLEM TO BE SOLVED: To store an electronic ticket to events
> provided at plural places on a single electronic device
> (smart card, portable computer, etc.), by allowing an
> electronic device to receive and store a place module that is
> related to each place where tickets are purchased.
> SOLUTION: An applet loader 102 loads one or more applets onto
> a smart card 100. An applet to be loaded enables the card 100
> to store a ticket to a place that is related to the loaded
> applet. A ticket loader 104 loads an electronic ticket to
> respective events onto the card 100. A ticket confirmation
> device 106 is located at a place where an event is held and a
> ticket to the event is stored in the card 100. The
> confirmation device 106 confirms the ticket so as to
> guarantee that the ticket is for the current event and
> receives the ticket based on this confirmation.
>

(19)日本国特許庁（ＪＰ）

(12) **公開特許公報（A）**

(11)特許出願公開番号
特開2000－57210
（P2000－57210A）

(43)公開日 平成12年２月25日(2000.2.25)

(51)Int.Cl.[7]	識別記号	FI	テーマコード（参考）
Ｇ０６Ｆ 17/60		Ｇ０６Ｆ 15/21	Ａ
// Ｇ０９Ｃ 1/00	６４０	Ｇ０９Ｃ 1/00	６４０Ｂ
	６６０		６６０Ａ
			６６０Ｂ

審査請求 未請求 請求項の数30 ＯＬ （全 16 頁）

(21)出願番号 特願平11－180905

(22)出願日 平成11年６月25日(1999.6.25)

(31)優先権主張番号 ０９／１０６．６００

(32)優先日 平成10年６月29日(1998.6.29)

(33)優先権主張国 米国（ＵＳ）

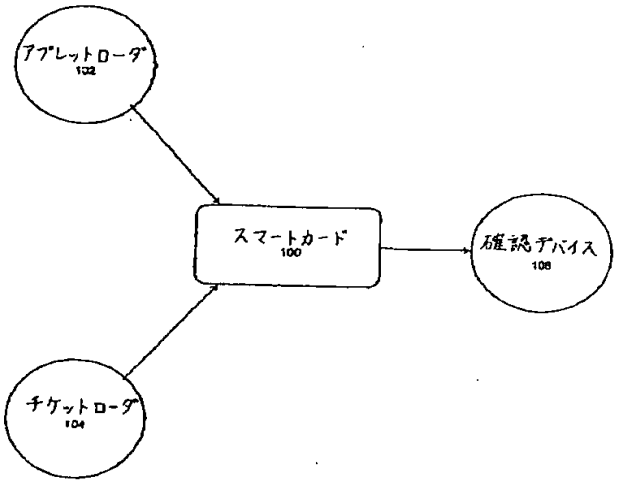
(71)出願人 595034134
サン・マイクロシステムズ・インコーポレイテッド
Ｓｕｎ Ｍｉｃｒｏｓｙｓｔｅｍｓ， Ｉｎｃ．
アメリカ合衆国 カリフォルニア州 94303 パロ アルト サン アントニオ ロード 901

(74)代理人 100078282
弁理士 山本 秀策

最終頁に続く

(54)【発明の名称】 スマートカードを用いた多開催地チケット発券

(57)【要約】
【課題】 単一の電子デバイス（スマートカード、および携帯コンピュータなど）上に複数の開催地で提供されるイベントに対する電子チケットを格納するためのシステムおよび方法が提供されること。
【解決手段】チケットを格納するために電子デバイスを使用する方法であって、第１の開催地に関連する第１の開催地モジュールを受信する工程であって、第１の開催地モジュールが第１の開催地に対するチケットを確認するための第１の開催地鍵を含む、工程と、第１の開催地モジュールを電子デバイスのモジュールローダ鍵を用いて確認する工程と、第１の開催地で提供されるイベントに対する第１のチケットを受信する工程と、第１のチケットに関連する第１のチケット署名を受信する工程と、第１のチケット署名を第１の開催地鍵を用いて認証する工程と、第１のチケットを第１の開催地の確認デバイスに提供する工程と、を包含する方法が提供される。



【特許請求の範囲】

【請求項１】 チケットを格納するために電子デバイスを使用する方法であって、

第１の開催地に関連する第１の開催地モジュールを受信する工程であって、該第１の開催地モジュールが該第１の開催地に対するチケットを確認するための第１の開催地鍵を含む、工程と、

該第１の開催地モジュールを該電子デバイスのモジュールローダ鍵を用いて確認する工程と、

該第１の開催地で提供されるイベントに対する第１のチケットを受信する工程と、

該第１のチケットに関連する第１のチケット署名を受信する工程と、

該第１のチケット署名を該第１の開催地鍵を用いて認証する工程と、

該第１のチケットを該第１の開催地の確認デバイスに提供する工程と、を包含する方法。

【請求項２】 第２の開催地に関連する第２の開催地モジュールを受信する工程であって、該第２の開催地モジュールが該第２の開催地のためのチケットを確認するための第２の開催地鍵を含む、工程と、

該第２の開催地モジュールを前記モジュールローダ鍵を用いて確認する工程と、

該第２の開催地で提供されるイベントのための第２のチケットを受信する工程と、

該第２のチケットを用いて第２のチケット署名を受信する工程と、

該第２のチケット署名を該第２の開催地鍵を用いて認証する工程と、をさらに包含する方法であって、

前記第１の開催地が該第２の開催地と異なる、請求項１に記載の方法。

【請求項３】 共有モジュールを受信する工程であって、該共有モジュールが前記第１の開催地モジュールによって使用される命令を含み、該第１の開催地モジュールを確認するための共有開催地鍵を有する、工程と、

該共有モジュールを前記モジュールローダ鍵を用いて確認する工程と、をさらに包含する請求項１に記載の方法。

【請求項４】 前記第１の開催地モジュールおよび前記共有モジュールの各々がモジュール署名を含み、前記確認する工程が前記確認されたモジュールの該モジュール署名を前記モジュールローダ鍵を用いて認証する工程を包含する、請求項３に記載の方法。

【請求項５】 前記第１の開催地モジュールを前記共有開催地鍵を用いて確認する工程をさらに包含する、請求項３に記載の方法。

【請求項６】 第１のチケットを受信する工程が、

チケットローダからのチャレンジを受信する工程と、

該チャレンジを前記第１の開催地鍵を用いて署名する工程と、

該署名されたチャレンジを該チケットローダに送信する工程と、を包含する、請求項１に記載の方法。

【請求項７】 第１の開催地モジュールを受信する工程が、

第１の開催地におけるイベントのためのチケットを処理するための第１の一連の命令を受信する工程と、

該第１の開催地のための第１の開催地鍵を受信する工程と、

該一連の命令を格納する工程と、

該一連の命令に関連する該第１の開催地鍵を格納する工程と、を包含する請求項１に記載の方法。

【請求項８】 共有モジュールが前記電子デバイス上に格納されているかどうかを判断する工程と、

該共有モジュールが該電子デバイス上に格納されていなければ、該共有モジュールを受信する工程と、をさらに包含する請求項７に記載の方法。

【請求項９】 前記共有モジュールを受信する工程が、

１つ以上の開催地モジュールによって使用される第２の一連の命令を受信する工程と、

該１つ以上の開催地モジュールを確認するための開催地ローダ鍵を受信する工程と、

該第２の一連の命令を格納する工程と、

該第２の一連の命令に関連する該開催地ローダ鍵を格納する工程と、を包含する、請求項８に記載の方法。

【請求項１０】 前記確認する工程が、前記第１の開催地モジュールのモジュール署名を前記電子デバイスのモジュールローダ鍵を用いて認証する工程を包含する、請求項１に記載の方法。

【請求項１１】 前記第１のチケットをキャンセルする工程をさらに包含する、請求項１に記載の方法。

【請求項１２】 前記第１のチケットをキャンセルする工程が該第１のチケットを無効にする工程を包含する、請求項１１に記載の方法。

【請求項１３】 前記共有モジュールを無効にする工程と、

新しいバージョンの該共有モジュールを受信する工程と、をさらに包含する、請求項１に記載の方法。

【請求項１４】 電子デバイス上で複数の開催地のためのチケットを維持する方法であって、

第１の開催地モジュールを格納する工程であって、該第１の開催地モジュールが第１の開催地と関連しそして第１の開催地鍵を含む、工程と、

チケットローダからチャレンジを受信する工程と、

該第１の開催地鍵を使用して、第１のデジタル署名を用いて該チャレンジを署名する工程と、

該署名されたチャレンジを該チケットローダに送信する工程と、

該第１の開催地におけるイベントに対する入場許可のための第１の電子チケットを受信する工程と、

第１のチケット署名を受信する工程であって、該第１の

チケット署名が該第１の電子チケットと関連する、工程と、
該第１の開催地鍵を用いて、該第１のチケット署名を認証する工程と、を包含する方法。
【請求項１５】　第２の開催地モジュールを格納する工程であって、該第２の開催地モジュールが第２の開催地と関連しそして第２の開催地鍵を含む、工程を、さらに包含する方法であって、
該第２の開催地が該第１の開催地と異なる、請求項１４に記載の方法。
【請求項１６】　前記第２の開催地におけるイベントに対する入場許可のための第２の電子チケットを受信する工程と、
第２のチケット署名を受信する工程であって、該第２のチケット署名が該第２の電子チケットと関連する、工程と、
前記第２の開催地鍵を用いて、該第２のチケット署名を認証する工程と、をさらに包含する請求項１５に記載の方法。
【請求項１７】　共有モジュールが格納されたかどうかを判断する工程であって、該共有モジュールが前記第１の開催地モジュールによって要求される命令を含む、工程と、
該共有モジュールが格納されていないならば、該共有モジュールを格納する工程と、をさらに包含する請求項１４に記載の方法。
【請求項１８】　チャレンジを受信する工程が生成された乱数を受信する工程を包含する、請求項１４に記載の方法。
【請求項１９】　第１の電子チケットを受信する工程が、前記第１の開催地におけるイベントの１つ以上の詳細を受信する工程を包含する、請求項１４に記載の方法。
【請求項２０】　チケットを提出する方法であって、該チケットが複数の開催地のためのチケットを格納することのできる電子デバイス上に格納され、
開催地において確認デバイスからチャレンジを受信する工程と、
第１の開催地鍵を使用して該チャレンジを署名する工程と、
該署名されたチャレンジを該確認デバイスに送信する工程と、
該開催地のおけるイベントのための第１のチケットに対する要求を受信する工程と、
該第１のチケットを送信する工程と、を包含する方法。
【請求項２１】　前記第１のチケットがキャンセルする工程をさらに包含する請求項２０の方法。
【請求項２２】　チャレンジを受信する工程が、生成された乱数を受信する工程を包含する、請求項２０に記載の方法。
【請求項２３】　前記第１のチケットを送信する工程が、前記イベントのための該第１のチケットを包含する１つ以上の詳細を送信する工程を包含する、請求項２０に記載の方法。
【請求項２４】　格納のためのメモリデバイスを備えるチケット格納装置であって、
第１の開催地におけるイベントのためのチケットを処理するための第１の開催地モジュールと、
該第１の開催地モジュールを確認するためのデバイス鍵と、
該イベントのための第１のチケットであって、該チケットがチケット署名を有する、第１のチケットと、
該チケット署名を認証するための開催地鍵と、
チケットローダおよび確認デバイスのうちの１つと該第１の開催地モジュールとのインターフェースをとるためのインターフェースモジュールであって、複数の開催地モジュール間で共有可能である、インターフェースモジュールと、を格納するためのチケット格納装置。
【請求項２５】　第２の開催地におけるイベントのためのチケットを処理するための第２の開催地モジュールをさらに備える請求項２４に記載の装置。
【請求項２６】　前記チケット格納装置がスマートカードを備える、請求項２４に記載の装置。
【請求項２７】　前記チケット格納装置が携帯コンピュータを備える、請求項２４に記載の装置。
【請求項２８】　チケットを格納するためのデータ構造を含むコンピュータ読み出し可能格納媒体であって、該データ構造が、
第１の開催地におけるイベントのためのチケットを処理するための第１の開催地モジュールと、
該第１の開催地モジュールを確認するためのデバイス鍵と、
該イベントのための第１のチケットであって、チケット署名を有する、第１のチケットと、
該チケット署名を認証するための開催地鍵と、
チケットローダおよび確認デバイスのうちの１つと該第１の開催地モジュールとのインターフェースをとるためのインターフェースモジュールであって、複数の開催地モジュール間で共有可能である、インターフェースモジュールと、を備える、コンピュータ読み出し可能格納媒体。
【請求項２９】　コンピュータによって実行される場合に、電子チケットを処理するための方法を該コンピュータに実行させる命令を格納するコンピュータ読み出し可能格納媒体であって、該方法が、
第１の開催地に関連する第１の開催地モジュールを受信する工程であって、該第１の開催地モジュールが該第１の開催地に対するチケットを確認するための第１の開催地鍵を含む、工程と、
該第１の開催地モジュールを該電子格納デバイスのモジ

ュールローダ鍵を用いて確認する工程と、
該第１の開催地で提供されるイベントに対する第１のチケットを受信する工程と、
該第１のチケットを用いて第１のチケット署名を受信する工程と、
該第１のチケット署名を該第１の開催地鍵を用いて認証する工程と、
該第１のチケットを該第１の開催地の確認デバイスに提供する工程と、を包含する、コンピュータ読み出し可能格納媒体。
【請求項３０】　複数の開催地におけるイベントのためのチケットを処理するための装置であって、
モジュールを受信するための受信手段であって、該モジュールがアプレットローダからのチケットを処理するための一連の命令を包含する、受信手段と、
該一連の命令を確認するためのモジュール確認手段と、
チケットローダからのチケットを受信するためのチケット受信手段と、
該チケットを確認するためのチケット確認手段と、
該チケットを確認デバイスに送信するための送信手段と、を備える装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子商取引の分野に関する。より詳しくは、電子チケット発券のためのシステムおよび方法を提供する。
【０００２】
【従来の技術】スポーツ開催、娯楽イベント、旅行などのためにチケットを使用することは、もはや厳密には機械的な機能ではない。チケット発券システムは、チケットの生成、発行、および確認作業のさまざまな段階においてコンピュータシステムを利用するように発展してきた。
【０００３】例えば、Ｂｅｒｓｏｎによって開示された、米国特許第５，５９８，４７７号において、顧客は、所望のチケットに関する情報（例えば、航空便に関する予定データ）を提出する。データ処理システムは、チケット発券情報および暗号化された確認データをローカル印刷システムに送信する。ローカルシステムは、２次元バーコード中に符号化された確認情報を含むチケットを印刷する。顧客は、航空便利用時刻にチケットを提示し、そこで確認システムは、チケットのバーコードをスキャンし、データを物理的形態からデジタル形態へ変換し、チケットを確認する。有効であるならば、顧客は、搭乗券および手荷物預かり証などを受け取る。
【０００４】
【発明が解決しようとする課題】しかし、Ｂｅｒｓｏｎのシステムは、紙のチケットの発行を依然必要とする。当然ながら、紙のチケットは、スリ、重複チケット発券、損壊、紛失などを被る。さらに、Ｂｅｒｓｏｎのシステムによって生成されるチケットは、必然的に１回限りの使用に適している。チケットは、航空便を利用するときに物理的に回収される。このシステムには、さらに２つの不利な点がある。第１に、２次元バーコードの使用は、そのようなバーコードを印刷することのできるプリンタおよびそのようなバーコードを読み取れることのできるバーコードスキャナを必要とする。チケットが印刷または受理される場所の数に依存して、これは著しいコストとなり得る。第２に、確認情報を安全にする暗号手段の使用では、高度な鍵管理システムを必要とする。
【０００５】Ｂｅｒｓｏｎシステムの変形においては、暗号によるセキュリティの代わりに大きな乱数が使用され得る。特定の乱数が選択され、物理的チケット上に１次元バーコードとして印刷される。大きな数を使用すると、別個のイベント（航空便、娯楽イベントなど）に対する特定のチケットに割り当てられる番号を人が正確に言い当てる確率は、著しく低下する。乱数は、チケットが使用される場所にアクセス可能なデータベース中に格納される。チケットがある場所で提示される場合、そのチケット上の番号は、データベース中に格納された有効番号のリストと比較される。このシステムは、損壊、重複チケット発券、および単一使用の制限などの紙のチケットに固有の不利な点を依然含んでいる。加えて、さらなる保護がなければ、乱数のデータベースは、一点の脆弱さを与える。データベースへアクセスを有する人が大量の偽のチケットをおそらく生成し得る。
【０００６】上記の不利な点に加えて、公知のチケット発券システムは、１つのイベントまたは１つの場所だけに対する入場を許可するものである。また、既知のシステムによって発行される紙のチケットは一般に、発行されたチケットを物理的に置き換えずには、変更されない。言い換えると、複数のイベントまたは複数の開催地を訪れたりまたは楽しんだりしたいと考える人は、各イベントまたは開催地に対する異なるチケットを持参し提示しなければならない。より多くのイベントまたは開催地を訪れる計画をすると、さらなる紙のチケットを購入し持参しなければならず、従って紛失の危険が大きくなる。
【０００７】従って、本発明の目的は、単一の電子デバイス（スマートカード、および携帯コンピュータなど）上に複数の開催地で提供されるイベントに対する電子チケットを格納するためのシステムおよび方法が提供されることである。
【０００８】
【課題を解決するための手段】本発明による方法は、チケットを格納するために電子デバイスを使用する方法であって、第１の開催地に関連する第１の開催地モジュールを受信する工程であって、該第１の開催地モジュールが該第１の開催地に対するチケットを確認するための第１の開催地鍵を含む、工程と、該第１の開催地モジュー

ルを該電子デバイスのモジュールローダ鍵を用いて確認する工程と、該第１の開催地で提供されるイベントに対する第１のチケットを受信する工程と、該第１のチケットに関連する第１のチケット署名を受信する工程と、該第１のチケット署名を該第１の開催地鍵を用いて認証する工程と、該第１のチケットを該第１の開催地の確認デバイスに提供する工程と、を包含する方法により、上記目的が達成される。

【００09】前記方法は、第２の開催地に関連する第２の開催地モジュールを受信する工程であって、該第２の開催地モジュールが該第２の開催地のためのチケットを確認するための第２の開催地鍵を含む、工程と、該第２の開催地モジュールを前記モジュールローダ鍵を用いて確認する工程と、該第２の開催地で提供されるイベントのための第２のチケットを受信する工程と、該第２のチケットを用いて第２のチケット署名を受信する工程と、該第２のチケット署名を該第２の開催地鍵を用いて認証する工程と、をさらに包含する方法であって、前記第１の開催地が該第２の開催地と異なってもよい。

【００１０】前記方法は、共有モジュールを受信する工程であって、該共有モジュールが前記第１の開催地モジュールによって使用される命令を含み、該第１の開催地モジュールを確認するための共有開催地鍵を有する、工程と、該共有モジュールを前記モジュールローダ鍵を用いて確認する工程と、をさらに包含してもよい。

【００１１】前記第１の開催地モジュールおよび前記共有モジュールの各々がモジュール署名を含み、前記確認する工程が前記確認されたモジュールの該モジュール署名を前記モジュールローダ鍵を用いて認証する工程を包含してもよい。

【００１２】前記方法は、前記第１の開催地モジュールを前記共有開催地鍵を用いて確認する工程をさらに包含してもよい。

【００１３】第１のチケットを受信する工程が、チケットローダからのチャレンジを受信する工程と、該チャレンジを前記第１の開催地鍵を用いて署名する工程と、該署名されたチャレンジを該チケットローダに送信する工程と、を包含してもよい。

【００１４】第１の開催地モジュールを受信する工程が、第１の開催地におけるイベントのためのチケットを処理するための第１の一連の命令を受信する工程と、該第１の開催地のための第１の開催地鍵を受信する工程と、該一連の命令を格納する工程と、該一連の命令に関連する該第１の開催地鍵を格納する工程と、を包含してもよい。

【００１５】前記方法は、共有モジュールが前記電子デバイス上に格納されているかどうかを判断する工程と、該共有モジュールが該電子デバイス上に格納されていなければ、該共有モジュールを受信する工程と、をさらに包含してもよい。

【００１６】前記共有モジュールを受信する工程が、１つ以上の開催地モジュールによって使用される第２の一連の命令を受信する工程と、該１つ以上の開催地モジュールを確認するための開催地ローダ鍵を受信する工程と、該第２の一連の命令を格納する工程と、該第２の一連の命令に関連する該開催地ローダ鍵を格納する工程と、を包含してもよい。

【００１７】前記確認する工程が、前記第１の開催地モジュールのモジュール署名を前記電子デバイスのモジュールローダ鍵を用いて認証する工程を包含してもよい。

【００１８】前記方法は、前記第１のチケットをキャンセルする工程をさらに包含してもよい。

【００１９】前記第１のチケットをキャンセルする工程が該第１のチケットを無効にする工程を包含してもよい。

【００２０】前記方法は、前記共有モジュールを無効にする工程と、新しいバージョンの該共有モジュールを受信する工程と、をさらに包含してもよい。

【００２１】電子デバイス上で複数の開催地のためのチケットを維持する方法であって、第１の開催地モジュールを格納する工程であって、該第１の開催地モジュールが第１の開催地と関連しそして第１の開催地鍵を含む、工程と、チケットローダからチャレンジを受信する工程と、該第１の開催地鍵を使用して、第１のデジタル署名を用いて該チャレンジを署名する工程と、該署名されたチャレンジを該チケットローダに送信する工程と、該第１の開催地におけるイベントに対する入場許可のための第１の電子チケットを受信する工程と、第１のチケット署名を受信する工程であって、該第１のチケット署名が該第１の電子チケットと関連する、工程と、該第１の開催地鍵を用いて、該第１のチケット署名を認証する工程と、を包含する方法により、上記目的が達成される。

【００２２】前記方法は、第２の開催地モジュールを格納する工程であって、該第２の開催地モジュールが第２の開催地と関連しそして第２の開催地鍵を含む、工程を、さらに包含する方法であって、該第２の開催地が該第１の開催地と異なってもよい。

【００２３】前記方法は、前記第２の開催地におけるイベントに対する入場許可のための第２の電子チケットを受信する工程と、第２のチケット署名を受信する工程であって、該第２のチケット署名が該第２の電子チケットと関連する、工程と、前記第２の開催地鍵を用いて、該第２のチケット署名を認証する工程と、をさらに包含してもよい。

【００２４】前記方法は、共有モジュールが格納されたかどうかを判断する工程であって、該共有モジュールが前記第１の開催地モジュールによって要求される命令を含む、工程と、該共有モジュールが格納されていないならば、該共有モジュールを格納する工程と、をさらに包含してもよい。

【００２５】前記方法は、チャレンジを受信する工程が生成された乱数を受信する工程を包含してもよい。

【００２６】前記方法は、第１の電子チケットを受信する工程が、前記第１の開催地におけるイベントの１つ以上の詳細を受信する工程を包含してもよい。

【００２７】チケットを提出する方法であって、該チケットが複数の開催地のためのチケットを格納することのできる電子デバイス上に格納され、開催地において確認デバイスからチャレンジを受信する工程と、第１の開催地鍵を使用して該チャレンジを署名する工程と、該署名されたチャレンジを該確認デバイスに送信する工程と、該開催地のおけるイベントのための第１のチケットに対する要求を受信する工程と、該第１のチケットを送信する工程と、を包含する方法により上記目的が達成される。

【００２８】前記方法は、前記第１のチケットがキャンセルする工程をさらに包含してもよい。

【００２９】チャレンジを受信する工程が、生成された乱数を受信する工程を包含してもよい。

【００３０】前記第１のチケットを送信する工程が、前記イベントのための該第１のチケットを包含する１つ以上の詳細を送信する工程を包含してもよい。

【００３１】格納のためのメモリデバイスを備えるチケット格納装置であって、第１の開催地におけるイベントのためのチケットを処理するための第１の開催地モジュールと、該第１の開催地モジュールを確認するためのデバイス鍵と、該イベントのための第１のチケットであって、該チケットがチケット署名を有する、第１のチケットと、該チケット署名を認証するための開催地鍵と、チケットローダおよび確認デバイスのうちの１つと該第１の開催地モジュールとのインターフェースをとるためのインターフェースモジュールであって、複数の開催地モジュール間で共有可能である、インターフェースモジュールと、を格納するためのチケット格納装置により、上記目的が達成される。

【００３２】前記装置は、第２の開催地におけるイベントのためのチケットを処理するための第２の開催地モジュールをさらに備えてもよい。

【００３３】前記チケット格納装置がスマートカードを備えてもよい前記チケット格納装置が携帯コンピュータを備えてもよい。

【００３４】チケットを格納するためのデータ構造を含むコンピュータ読み出し可能格納媒体であって、該データ構造が、第１の開催地におけるイベントのためのチケットを処理するための第１の開催地モジュールと、該第１の開催地モジュールを確認するためのデバイス鍵と、該イベントのための第１のチケットであって、チケット署名を有する、第１のチケットと、該チケット署名を認証するための開催地鍵と、チケットローダおよび確認デバイスのうちの１つと該第１の開催地モジュールとのインターフェースをとるためのインターフェースモジュールであって、複数の開催地モジュール間で共有可能である、インターフェースモジュールと、を備える、コンピュータ読み出し可能格納媒体により、上記目的が達成される。

【００３５】コンピュータによって実行される場合に、電子チケットを処理するための方法を該コンピュータに実行させる命令を格納するコンピュータ読み出し可能格納媒体であって、該方法が、第１の開催地に関連する第１の開催地モジュールを受信する工程であって、該第１の開催地モジュールが該第１の開催地に対するチケットを確認するための第１の開催地鍵を含む、工程と、該第１の開催地モジュールを該電子格納デバイスのモジュールローダ鍵を用いて確認する工程と、該第１の開催地で提供されるイベントに対する第１のチケットを受信する工程と、該第１のチケットを用いて第１のチケット署名を受信する工程と、該第１のチケット署名を該第１の開催地鍵を用いて認証する工程と、該第１のチケットを該第１の開催地の確認デバイスに提供する工程と、を包含する、コンピュータ読み出し可能格納媒体により、上記目的が達成される。

【００３６】複数の開催地におけるイベントのためのチケットを処理するための装置であって、モジュールを受信するための受信手段であって、該モジュールがアプレットローダからのチケットを処理するための一連の命令を包含する、受信手段と、該一連の命令を確認するためのモジュール確認手段と、チケットローダからのチケットを受信するためのチケット受信手段と、該チケットを確認するためのチケット確認手段と、該チケットを確認デバイスに送信するための送信手段と、を備える装置により、上記目的が達成される。

【００３７】本発明の１つの実施態様において、単一の電子デバイス（スマートカード、および携帯コンピュータなど）上に複数の開催地で提供されるイベントに対する電子チケットを格納するためのシステムおよび方法が提供される。この実施態様において、電子デバイスは、チケットが購入される各開催地に関連した開催地モジュールを受信し格納する。開催地モジュールは、電子デバイスが、関連した開催地に対するチケットを格納することを可能にし、また個々のチケットを確認するための開催地鍵を含む。電子デバイスはまた、１つ以上の開催地モジュールによって要求される命令を含むチケット発券共有モジュールを受信し格納する。チケット発券共有モジュールは、インストールされた開催地モジュールを確認するための「開催地ローダ鍵」を含む。

【００３８】電子デバイスがチケット発券共有モジュールおよび１つ以上の開催地モジュールを用いて構成された後に、各インストールされた開催地モジュールに対するチケットが格納され得る。本発明の本実施態様において、電子デバイスのユーザは、チケットに対するパラメ

ータ（イベント、日付、時刻、座席など）を特定し、対応する電子チケットがチケット署名とともにチケットローダからダウンロードされる。対応する開催地モジュールに対する開催地モジュールは、その開催地鍵を使用して、各格納されたチケットの署名を認証する。

【００３９】チケットがイベントへの入場許可のために提示されるものである場合、本実施態様においては、確認デバイスがチャレンジコードを発行することによって電子デバイスをチャレンジする。イベントの開催地に対する開催地モジュールは、開催地鍵を用いてそのコードを署名し、署名されたコードを返信する。署名が確認された後に、電子デバイスはイベントに対するチケットを転送し、チケットはキャンセルされる。

【００４０】

【発明の実施の形態】以下の記載により、当業者は、本発明を作成および使用することができる。以下の記載は、特定の用途およびその要求にしたがって与えられる。本発明は、本明細書中で示される実施態様に限定されるように意図されないが、本明細書中で開示される原理および特徴に整合する最も広い範囲に従うものである。

【００４１】例えば、本発明の本実施態様において、暗号手段は、スマートカード上にロードされる電子チケットおよび開催地モジュールまたはアプレット（小規模Ｊａｖａアプリケーションなど）の安全性を確実にするために用いられる。当業者は、以下に記載される暗号鍵の目的が、スマートカード上に格納された情報の安全性および認証性を確実にするためであり、特に指摘しなければ必ずしも特定の暗号システムに依存しないことを理解する。したがって、種々の暗号鍵は、種々の目的のために以下に記載される。しかし、本発明は、暗号の安全性のための特定の方法に限定されず、本発明の特定の実施態様は、非対称鍵システム、対象鍵システム、または工夫され得るようないくつかの他のシステムを使用し得る。

【００４２】本発明の１つの実施態様によると、複数の開催地に対する電子チケットを生成、格納、および確認するためのシステムおよび方法が与えられる。チケットは、例示的に標準的スマートカード上に格納されるが、３ＣＯＭ　ＣｏｒｐｏｒａｔｉｏｎによるＰａｌｍＰｉｌｏｔまたはＤａｌｌａｓ　ＳｅｍｉｃｏｎｄｕｃｔｏｒによるｉＢｕｔｔｏｎなどの他のデバイスも意図される。格納されたチケットは、スポーツイベント、娯楽イベント、航空便、および自動車通行料などの、入場券または通行券が予め購入され得る任意の機会に対するものであり得る。本発明の本実施態様によりチケットがスマート上に格納された各開催地は、スマートカード上に格納された関連アプレットを有する。チケット発券共有アプレットがまた格納される。以下に記載されるように、これらのアプレットは、スマートカードとチケット／開催地ロード機能との間およびスマートカードとチケット確認デバイスとの間のインターフェースをとるために使用される。

【００４３】図１は、ユーザのスマートカード上に格納されたチケットを発行、格納、および確認するための本発明の実施態様による例示的システムを図示する。スマートカード１００は、スマートカードに対するＩＳＯ７８１６仕様に例示的に従う。このようなスマートカードは、後に取り出されるための電子データの種々の種類および量を格納することができる。

【００４４】アプレットローダ１０２は、スマートカード１００上へ１つ以上のアプレットをロードする。アプレットローダ１０２によってスマートカード１００上へロードされるアプレットは、スマートカード１００がロードされたアプレットに関連した開催地へのチケットを格納することを可能にする。例えば、１つの開催地アプレットは、Ｓａｎ　Ｆｒａｎｃｉｓｃｏ　Ｇｉａｎｔｓによって開催される野球の試合に対応し得る。このアプレットをロードすることは、スマートカード１００が特定の試合またはある範囲の試合（例えば、シーズンパス）に対するチケットを格納することを可能にする。例示的に、アプレットローダ１０２は、単一開催地に関するアプレットをロードするように構成される。しかし、別の実施態様において、アプレットローダ１０２は、複数の開催地からアプレットをロードする。

【００４５】開催地アプレット（すなわち、個々の開催地に関連したアプレット）に加えて、チケット発券共有アプレットがまた、すべての開催地アプレットによって使用されるためにスマートカード１００上へロードされる。以下に議論されるように、この共有アプレットは、開催地アプレットの各々に共通して利用可能であり、開催地アプレットの各々に代わって使用される機能を与える。

【００４６】チケットローダ１０４は、個々のイベント（またはある範囲のイベント）に対する電子チケットをスマートカード１００上へロードする。各スマートカードは、同じまたは異なるイベント、開催地、および日付などに対する複数のチケットを格納することができる。例示的に、スマートカード１００上へロードされた各チケットは、イベントを開催しチケットを受理する開催地に対応する開催地アプレットに関連して格納される。本実施態様において、開催地のアプレットは、その開催地でのイベントに対するチケットがロードされる前にスマートカード１００上へ（アプレットローダ１０２などによって）ロードされる。

【００４７】例示的に、チケット確認デバイス１０６は、イベントを開催する開催地に位置し、そのイベントに対するチケットがスマートカード１００に格納される。確認デバイス１０６は、チケットが現在のイベントに対するものであることを保証するようにチケットを確

認し、この確認に基づいてチケットを受信する。

【0048】本発明の本実施態様において、アプレットローダ102、チケットローダ104、および確認デバイス106は、スマートカード100を受信、読み取り、および書き込みするために備えられた別個の電子システムである。この実施態様において、ユーザは、所望の処理を行うために各システムにスマートカード100を物理的に提示する。別の実施態様において、アプレットローダ102、チケットローダ104、および確認デバイス106のいずれかまたはすべてが同じシステムに配置する。特に、アプレットローダおよびチケットローダがそうである。

【0049】本発明のさらに別の実施態様において、アプレットローダ102、チケットローダ104、および確認デバイス106のいずれかまたはすべてがインターネットまたは他のワイドエリアネットワークに接続されたコンピュータシステムを備える。このような実施態様において、これらのシステムは、スマートカード100を受信、読み取り、および書き込みするために備えられたユーザのコンピュータシステムを介してユーザによってアクセスされる。

【0050】図2は、チケット発券共有アプレット、複数の開催地アプレット、および複数のチケットが存在するスマートカード100を図示する。スマートカード100は、他のデバイス(図1のアプレットローダ102、チケットローダ104、および確認デバイス106など)とインターフェースをとり、スマートカードからの情報の取り出しおよび格納を管理するためのオペレーティングシステム200を備える。オペレーティングシステム200は、例示される実施態様において、ロードされたアプレットを動作させるためのJava Virtual Machine(JVM)を含む。オペレーティングシステム200は、スマートカード100上へロードされたアプレットを確認するための暗号鍵200a(以下「アプレットローダ鍵」と称される)をさらに含む。したがって、アプレット署名202b、210b、および220bは、アプレットがロードされたときに、アプレットローダ鍵200aを用いて認証される。例示的に、アプレット署名は、関連したアプレットのロードの前またはそれと同時に作成される。

【0051】チケット発券共有アプレット202は、スマートカード100上にインストールされた種々の開催地アプレットによって要求される命令(例えば、モジュール、オブジェクト、およびファンクションなどの形態をとる)を含む。チケット発券共有アプレット202は、各開催地アプレットに共通の機能(チケット確認、チケットローダ104および確認デバイス106と通信するためのプロトコルなど)を与え、したがって各開催地アプレットのサイズがより小さくなることを可能にし、従ってスマートカード100上に格納領域を確保できる。例えば、本発明の1つの実施態様において、チケット発券共有アプレット202は、チケットをロード、確認、および/またはキャンセル(例えば、イベントへの入場許可を得るためにチケットが使用された後のキャンセル)をするための命令を与える。チケット発券共有アプレット202は、以下で記述されるように、個々の開催地アプレットを確認するために暗号鍵202a(以下「開催地ローダ鍵」と称される)を含む。特に、開催地アプレットがロードされたとき、チケット発券共有アプレット202は、各アプレットの開催地署名を認証する。

【0052】本発明の別の実施態様において、チケット発券共有アプレットは、チケットの詳細を遵守することを強制または確実にするための命令を含む。例えば、このような実施態様において、スマートカード100は、ユーザがチケットで決められた自分の座席に座っていることを確かめたり、または正しい座席を見つけることを補助するためにイベントにおける客席区域内に配置されるスマートカード読み取り器に挿入され得る。

【0053】開催地アプレット210および220は、スマートカード100上にインストールされている様子が示される。例示的に、開催地アプレット210は、SanFrancisco Giantsのホームでの野球の試合を表す。開催地アプレット220は、例示的にUnited Airlinesの航空便を表す。開催地アプレット210および220は、チケットをロードする前にチケットローダ104に対し開催地アプレット210および220を認証するために使用される暗号鍵210aおよび220a(以下「開催地鍵」と称される)を含む。開催地鍵はまた、関連した開催地に対する、チケットに伴うチケット署名を確認するために使用される。

【0054】開催地アプレット210および220はまた、オペレーティングシステム200に対し開催地アプレットを確認するためのアプレット署名210bおよび220bを含む。上述のように、例示的に、アプレット署名は、開催地アプレットのロードの前にまたはそれと同時にアプレットローダ102によって作成される。次にオペレーティングシステム200は、アプレットがロードされたときに、アプレットローダ鍵200aを用いてアプレット署名210bおよび220bを認証する。

【0055】開催地アプレット210および220は、チケット発券共有アプレットに対し開催地アプレットを確認するための開催地署名210cおよび220cをさらに含む。アプレット署名210bおよび220bと同様に、開催地署名210cおよび220cは、開催地アプレット210および220のインストールの前にまたはそれと同時に作成される。開催地アプレットがロードされたとき、チケット発券共有アプレット202は、開催地署名を認証する。

【００５６】チケット２１２、２１４、および２１６は、San Francisco Giantsのホームで行われる特定の野球の試合を表す。チケット２２２は、San FranciscoからPittsburgh、PAへのUnitedAirlinesにより提供される特定の航空便を表す。

【００５７】スマートカード１００上に格納された各チケットは、関連イベントに関する情報を含む。したがって、チケット２１２、２１４、および２１６は、試合の日付、対戦相手、および指定座席番号などの情報を含む。本発明の本実施態様において、チケット中に格納された情報は、チケットの認証を確認するためにチケット署名とともに使用される。したがって、チケットに格納された情報の量および種類は、開催地、イベント、およびチケットの種類などに依存して変化する。個々のチケット２１２、２１４、および２１６の代わりに、スマートカード１００の所有者は、例えば、シーズンパスの形態の唯一のチケットを有することがある。シーズンパスチケットは、１日を越えて有効であり、したがってチケット２１２、２１４、および２１６と異なる情報を含む。

【００５８】チケット２１２、２１４、２１６、および２２２はそれぞれ、対応する開催地の鍵を用いてチケットローダ１０４によって生成されたチケット署名（参照符号２１２ａ、２１４ａ、２１６ａ、および２２２ａによって表される）を含む。公開鍵暗号（ＰＫＥ）および非対称鍵ペアを用い、開催地鍵２１０ａおよび２２０ａが開催地公開鍵である本発明の実施態様において、チケット署名は、公開鍵に対応する秘密鍵を使用して生成される。対象鍵（ＤＥＳなど）を使用する別の実施態様において、チケットローダ１０４は、開催地鍵２１０ａおよび２２０ａのコピーを用いて、発行されたチケットの署名をする。上記のように、チケットがスマートカード１００上へロードされたとき、対応する開催地アプレットは、チケット署名をその開催地鍵を用いて認証することによってチケットを確認する。

【００５９】当業者は、スマートカード１００上に格納されたアプレットが、データの秘密を保持し得、したがって他の格納されたアプレットへアクセス不可能であることを理解する。これは、１つのアプレットが、特定の開催地アプレットと関連したチケットに不正を働いたり、または検査したりすることを防止する。しかし、本実施態様において、チケットは、確認デバイス１０６に提示された後にキャンセルまたは使用不可にされる。別の実施態様において、個々のチケットは、削除または上書きされる。

【００６０】アプレットのロード

本発明の本実施態様において、スマートカード１００上にロードされる開催地アプレットおよびチケット発券共有アプレットは、実行可能なコンピュータプログラムまたは実行可能なコンピュータコードのモジュールを含む。本発明の本実施態様において、チケット発券共有アプレットは、スマートカード間で実質的に同一である。各開催地の開催地アプレットは同様に、開催地鍵およびロードされ得る任意のチケットを除いて、スマートカード間で同様である。

【００６１】本発明の１つの実施態様において、開催地アプレットは、標準的な方法によって構成されたＪａｖａアプリケーションを含む。例えば、Ｊａｖａプログラミング命令を含むファイルは、バイナリクラスファイルを形成するためにＪａｖａコンパイラを用いてコンパイルされる。次に、クラスファイルは、スマートカードアプリケーションファイルに変換される。この変換プロセス中に、カードアプリケーションファイルは、暗号化の種類（例えば、対称または非対称）に依存して、アプレットローダ鍵２００ａ（図２に示す）またはその相補形を使用してデジタル的に署名される。

【００６２】図３は、署名されたカードアプリケーションファイル（例えば、図２のアプレット２１０）がアプレットローダ１０２からスマートカード１００上へロードされる例示的なプロセスを図示する。本発明の本実施態様において、アプレットローダ１０２は、チケット販売機であり、チケットローダ１０４と同じ場所に配置される。この実施態様において、開催地アプレット２１０は、Ｇｉａｎｔｓの野球チケットが購入されたときに、アプレットがまだスマートカード１００上になければ、自動的にロードされる。また、この実施態様において、チケット発券共有アプレット２０２は、スマートカード１００上になければ自動的にロードされる。別の実施態様において、チケット発券共有アプレット２０２および開催地アプレット２１０のいずれか一方または両方が、スマートカードが製造される時点またはそれが販売される時点で、スマートカード上に予めロードされる。

【００６３】ここで図３を参照すると、状態３００は開始状態である。状態３０２において、アプレットローダ１０２は、スマートカード１００に結合され、アプレット２１０をダウンロードする準備をする。例示的に、スマートカード１００の所有者は、アプレットローダ１０２を含むデバイスへスマートカードを挿入し、アプレット２１０のインストールを選択する（例えば、Ｇｉａｎｔｓの野球チケットの購入を希望することによって）。別の実施態様において、所有者は、インターネットまたは他の通信リンクを介してアプレットローダ１０２に接続された別個のコンピュータシステムにスマートカード１００を挿入する。

【００６４】状態３０４において、スマートカード１００は、アプレットをロードする準備がなされたことを示し、そして、本実施態様においては、現在の構成に関する情報（どのアプレットがロードされるか、どのバージョンのオペレーティングシステムおよびＪａｖａ Ｖｉ

rtual Machineがインストールされるかなどの情報）をアプレットローダに渡す。１つの実施態様において、スマートカード１００は、アプレットを受信する用意ができたことを示す前に自己チェックを行う。例示的に、自己チェックは、データを格納および取り出すカードの能力を試験し、不良なまたは損壊のあるメモリセルを試験する。スマートカードによってアプレットローダ１０２へ転送された情報は、カード上で利用できる格納領域の量を含み得る。選択されたアプレットをロードするための領域が不十分な場合、エラーメッセージがユーザに示される。

【００６５】状態３０６において、アプレットローダ１０２は、チケット発券共有アプレット２０２がすでにスマートカード１００上に存在するかどうかを判断する。上記のように、チケット発券共有アプレット２０２は、開催地アプレット２１０および他の開催地アプレットによって使用される命令を含む。例示的に、この判断は、状態３０４においてスマートカード１００によってアプレットローダ１０２へ返された情報に基づいてなされる。

【００６６】状態３０６においてチケット発券共有アプレット２０２がスマートカード１００上にインストールされていないと判断される場合、プロセスは、状態３１０へ続く。そうでない場合は、状態３０８において開催地アプレット２１０がすでにスマートカード１００上にロードされているかどうか判断される。ロードされていなければ、プロセスは、状態３１６に進む。しかし、両方のアプレットがすでにロードされていれば、プロセスは終了状態３２０へ進む。

【００６７】状態３１０において、チケット発券共有アプレットは、まだ署名されていなければ、アプレットローダ鍵２００ａに相補的な暗号鍵（例えば、非対称暗号システムを使用する場合、「秘密」鍵は「公開」鍵２００ａに対応する）を用いて署名され（例えば、アプレットローダ１０２によって）、アプレット署名２０２ｂ（図２参照）を作成する。次に、署名されたアプレットは、スマートカード１００にダウンロードされる。例示的に、アプレットは、何バイトかの複数のストリーム（例えば、各ストリーム中約２００バイト）でスマートカード上にダウンロードおよび格納され、各ストリームは、関連したチェックサムによって確認される。状態３１２において、スマートカードは、アプレットの正確な受信を確認し、状態３１４においてインストールが成功したかしていないかをアプレットローダに通知する。共有アプレット２０２が正しくロードされていなかったならば、エラーメッセージが返され、プロセスは、終了状態３２０で終了する。

【００６８】チケット発券共有アプレット２０２のインストールが成功すれば、または開催地アプレット２１０がロードされていないと状態３０８において判断されるならば、プロセスは状態３１６に進む。

【００６９】状態３１６において、開催地アプレット２１０は、アプレットローダ１０２によって署名され（まだ署名されていなければ）、アプレット署名２１０ｂおよび／または開催地署名２１０ｃを作成し、そして次にアプレットローダ１０２からスマートカード１００上へダウンロードされる。以下に議論されるように、開催地鍵２１０ａは、チケットローダ１０４に対する開催地アプレット２１０を認証するためおよびチケットローダからロードされたチケットを確認するために使用される。好ましい暗号安全性の種類（例えば、対称または非対称鍵）に依存して、アプレット署名２１０ｂおよび開催地署名２１０ｃは、アプレットローダ鍵２００ａおよび開催地ローダ２０２ａ、またはその相補形をそれぞれ用いて作成される。

【００７０】状態３１８において、スマートカード１００は、ダウンロードされたアプレットを確認し、アプレットのロードが成功したかまたはエラーが起きたかをアプレットローダに示す。例示的に、スマートカード１００は、チェックサムを計算しそれをアプレットローダ１０２によって与えられたチェックサムと比較することによってアプレットの受信が成功したことを確認する。別の実施態様において、ダウンロードされたアプレットのアプレット署名２１０ｂは、署名の作成に使用された鍵の形態に対応する暗号技術を用いて確認される。１つの特定のこのような実施態様において、スマートカード１００は、アプレットからのハッシュ値を計算し、その値と署名から取り出されたハッシュ値とを比較する。この２つのハッシュ値が一致すれば、スマートカードはアプレットが完全な状態で受信されたと考える。同様のプロセスを使用して、チケットがダウンロードされた場合にチケット署名を確認する。次いでプロセスは、終了状態３０２で終了する。

【００７１】チケットのロード

一旦開催地アプレットがスマートカード１００上へロードされると、その開催地でのイベント（スポーツ競技場での競技または試合、航空会社によって提供される航空便など）に対するチケットは購入され、同様にロードされ得る。本発明の本実施態様において、開催地アプレット、チケット発券共有アプレット２０２、および関連チケットは、互いに併せあって、組合わせられたチケット／アプレットローダから必要に応じてロードされる。

【００７２】図4は、チケットローダ１０４からＧｉａｎｔｓの野球の試合（これのための開催地アプレット２１０がインストールされている）に対する電子チケットを購入し、電子チケットをスマートカード１００上にインストールするための例示的な手続きを図示する。本発明の本実施態様において、チケットローダ１０４は、インターネットなどの公衆通信回線に接続されたウエブサーバの一部である。この実施態様において、スマートカ

ード１００は、スマートカード１００の所有者によって操作されるコンピュータシステムに結合される。このコンピュータシステムはまた、インターネットに接続される。チケットは、開催地のウエブサーバに対するインターフェースを使用して選択され、次にインターネットを介してダウンロードされ、スマートカード１００上に格納される。

【００７３】ここで図４を参照すると、状態４００が開始状態である。状態４０２において、スマートカード１００の所有者は、チケット購入／ロード手続きを開始する。本発明の１つの実施態様において、所有者は、第１に、チケットを希望するイベントを選択する。ここで記述の実施態様において、例えば、野球の試合は、所望の座席の番号および種類とともに特定される。別の例として、所有者は、航空路線予約代理人に対して所有者が搭乗を希望する航空便（日付、時刻、およびおそらく座席を含む）を特定する。スマートカードの所有者が開催地／イベントを選択し、そのイベントに関する任意の必要事項または基準を特定した後に、所有者は、そのように構成されたチケットの受信を合図する。

【００７４】状態４０４において、チケットローダ１０４は、スマートカードおよび／または開催地アプレット２１０を認証するために、自分自身を識別し、スマートカード１００にチャレンジする。例示的に、チャレンジは、チケットローダ１０４によってスマートカード１００へ送信された乱数の形態をとる「ゼロ知識証明（ｚｅｒｏ ｋｎｏｗｌｅｄｇｅ ｐｒｏｏｆ）」である。開催地アプレット２１０は、開催地鍵２１０ａ用いてデジタル署名を生成し、そして結果をチケットローダ１０４に戻すことによってチャレンジを満たす。別の実施態様において、開催地アプレット２１０は、開催地鍵２１０ａを用いて乱数を暗号化し、そして結果をチケットローダ１０４に戻すことによって、状態４０６においてチャレンジを満たす。

【００７５】状態４０８において、チケットローダ１０４は、スマートカード１００から受け取られた署名を確認する。この確認の目的のために、チケットローダ１０４は、開催地鍵２１０ａに対して相補形の鍵を有する。例えば、開催地鍵２１０ａが関連する開催地の公開鍵である、非対称鍵（例えば、ＲＳＡ）を使用する本発明の実施態様において、チケットローダ１０４は、対応する秘密鍵を有する。対称鍵（例えば、デジタル暗号基準）を使用する本発明の実施態様において、チケットローダ１０４および開催地アプレット２１０は、同じ鍵のコピーを有する。確認の試みが失敗すれば、チケットロードプロセスは、実施および安全性の関係に依存して、チャレンジ／確認手続きを再度試みるか（制限回数まで）、または失敗しそしてエラーを報告するかのいずれかを行う。

【００７６】次に、状態４１０において、チケットローダ１０４は、スマートカードの所有者／ユーザによって選択されたイベントデータに基づいて開催地に対するチケット２１２を生成および署名する。例示的に、チケットローダ１０４は、開催地アプレット２１０が状態４０８において確認されたのと同じ鍵を使用してチケット２１２に署名する。状態４１２において、署名２１２ａで署名を完了したチケット２１２が、スマートカード１００上にダウンロードおよび格納される。

【００７７】状態４１４において、開催地アプレット２１０は、開催地鍵２１０ａを用いて署名２１２ａを認証することによって、ダウンロードされたチケット２１２を確認し、そして状態４１６において、成功または失敗を示すメッセージを用いて応答する。本発明の別の実施態様において、開催地鍵２１０ａと異なる第２の開催地鍵が、ダウンロードされたチケットを確認する目的のために開催地アプレット２１０とともに格納される。手続きは、終了状態４１８で終了する。

【００７８】ここで記述の実施態様において、上記プロセスに続いて、各チケットがチケットローダ１０４からダウンロードされなければならない。別の実施態様において、複数のチケットが、一度に１つの開催地に対して、選択、処理、およびダウンロードされ得る。

【００７９】チケット確認

本発明の本実施態様において、チケットは、適切な開催地での受信のために提示される場合に、確認デバイス１０６によって確認される。図５は、本発明の本実施態様による、チケット２１２を確認するための例示的手続きを図示する。

【００８０】状態５００は、開始状態である。状態５０２において、ユーザは、チケット２１２において特定される野球の試合への入場許可を得るために、スマートカード１００を確認デバイス１０６へ提示する。例示的に、確認デバイス１０６は、スマートカード１００を受け取り、それと通信するように構成されたコンピュータシステムを含む。

【００８１】状態５０４において、確認デバイス１０６は、上記チケットロード手続きにおいて行われたように、スマートカード１００に対するチャレンジを生成および発行する。スマートカード１００に与えられる乱数は、状態５０６において、開催地鍵２１０ａを使用して、開催地アプレット２１０によって署名される。状態５０８において、確認デバイスが開催地鍵２１０ａに相補形の鍵を使用して署名を認証する。チャレンジとともに戻された署名を認証することによって、確認デバイス１０６は、開催地アプレット２１０を確認できる。

【００８２】署名を認証した後に、状態５１０において、確認デバイス１０６は、スマートカード１００によって保持されるチケットデータを要求する。開催地アプレット２１０は、状態５１２において、チケット２１２（例えば、チケットデータおよび署名）を確認デバイス

１０６に送信する。例示的に、確認デバイス１０６は、日付、時刻、および／または他の識別データによって識別される、現在のイベントに対して使用可能な格納されたチケットだけが通知される。本発明の１つの実施態様において、チケット発券共有アプレット２０２は、確認デバイス１０６に対して特定されるチケットを決定する（例えば、どの開催地－したがってどの開催地アプレットおよびチケット－が確認デバイスに対応するかを決定することによって）。あるいは、開催地アプレット２１０および確認デバイス１０６は、現在の開催地に関連した複数のチケットのうちのどれが使用されるべきかを決定するために、通信する。

【００８３】状態５１４において、確認デバイス１０６は、チケットデータを確認し（例えば、日付、時刻、参加チーム、および座席番号を確かめる）、チケット署名を認証する。チケットデータおよび署名が検査を通過すれば、スマートカード１００は、チケット２１２をキャンセルまたは消去するように命令され、ユーザは許可される。

【００８４】本発明のここで記述の実施態様において、チケット２１２は、スマートカード１００上にロードされた将来のチケットを用いて上書きされる。別の実施態様において、チケットは、消去も上書きもされない。

【００８５】１つのスマートカード上にある複数の開催地のための電子チケットを格納および確認するためのシステムおよび方法が提供される。本実施態様によると、スマートカードのオペレーティングシステムは、Ｊａｖａ Ｖｉｒｔｕａｌ Ｍａｃｈｉｎｅおよびアプレットローダ鍵を含む。開催地ローダ鍵を含む共有アプレットは、アプレットローダ鍵を用いて確認され、スマートカード上に格納される。１つ以上の開催地アプレットがまた、関連する開催地に対応するそれぞれの開催地鍵とともにスマートカード上に格納される。各開催地アプレットは、アプレットローダ鍵および開催地ローダ鍵によって確認される。共有アプレットは、チケットローダおよびチケット確認デバイスとのインターフェースをとるために開催地アプレットによって使用される。チケットは、開催地アプレットに関連するイベントに対して購入され、関連する開催地アプレットに関連してスマートカード上に格納される。チケット署名は、各開催地アプレット開催地鍵を用いて認証される。チケットは、イベントへの入場許可を得るために提出された後にキャンセルされる。

【００８６】本発明の実施態様の前述の記載は、例示および説明だけの目的で提示された。例示および記載は、あらゆる実施例を説明し尽くすものでもなければ、本発明を開示された形態に限定することを意図しない。多くの改変および変更が当業者にとって明らかである。したがって、上記開示は本発明を限定することを意図せず、本発明の範囲は、添付の請求の範囲によって規定される。

【００８７】

【発明の効果】単一の電子デバイス（スマートカード、および携帯コンピュータなど）上に複数の開催地で提供されるイベントに対する電子チケットを格納するためのシステムおよび方法が提供される。これにより、紙のチケットの発行を必要がなくなり、さらに、多くのイベントに参加する場合、多くの紙のチケットを持参する必要がなくなる。

【図面の簡単な説明】

【図１】スマートカードが開催地アプレットおよび開催地への入場のためのチケットを格納するために使用される、本発明の実施態様によるシステムを図示する１つのブロック図である。

【図２】複数の開催地アプレットおよびチケットを含む、本発明の実施態様によるスマートカードを図示する図である。

【図３】スマートカード上に開催地アプレットをロードする、本発明の実施態様による１つの方法を示すフローチャートである。

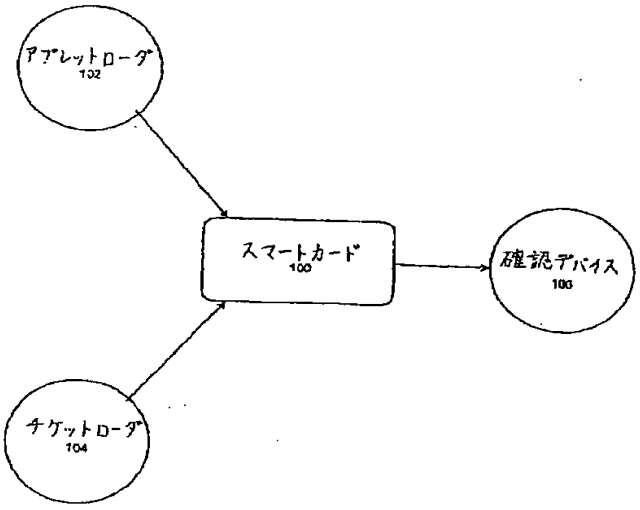
【図４】スマートカード上にチケットをロードする、本発明の実施態様による１つの方法を示すフローチャートである。

【図５】スマートカード上に格納されたチケットを確認する、本発明の実施態様による１つの方法を示すフローチャートである。

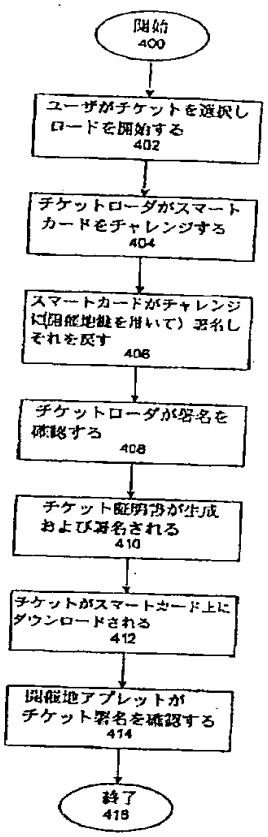
【符号の説明】

１００　スマートカード
１０２　アプレットローダ
１０４　チケットローダ
１０６　確認デバイス

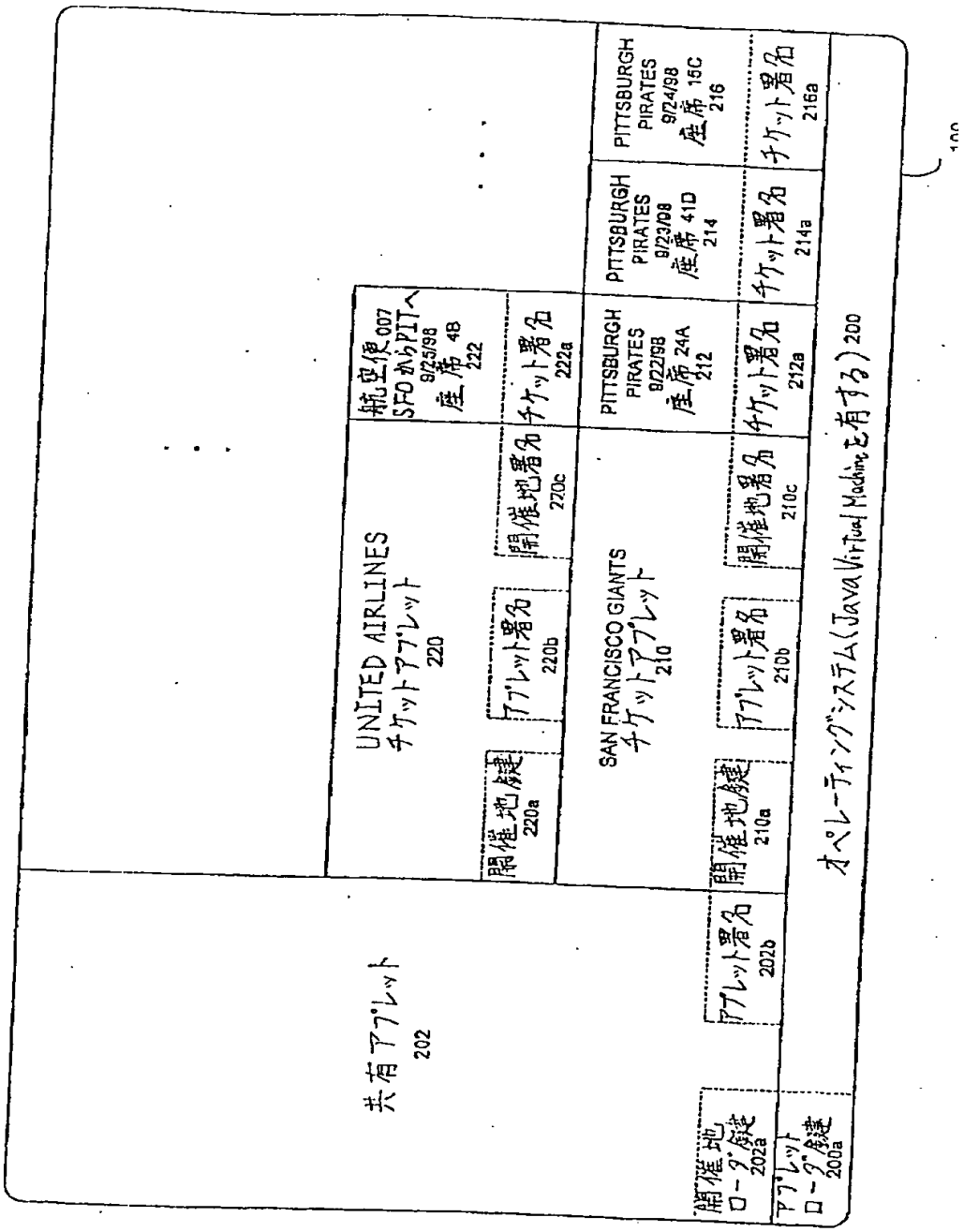
【図1】


アプレットローダ
102
スマートカード
100
確認デバイス
106
チケットローダ
104

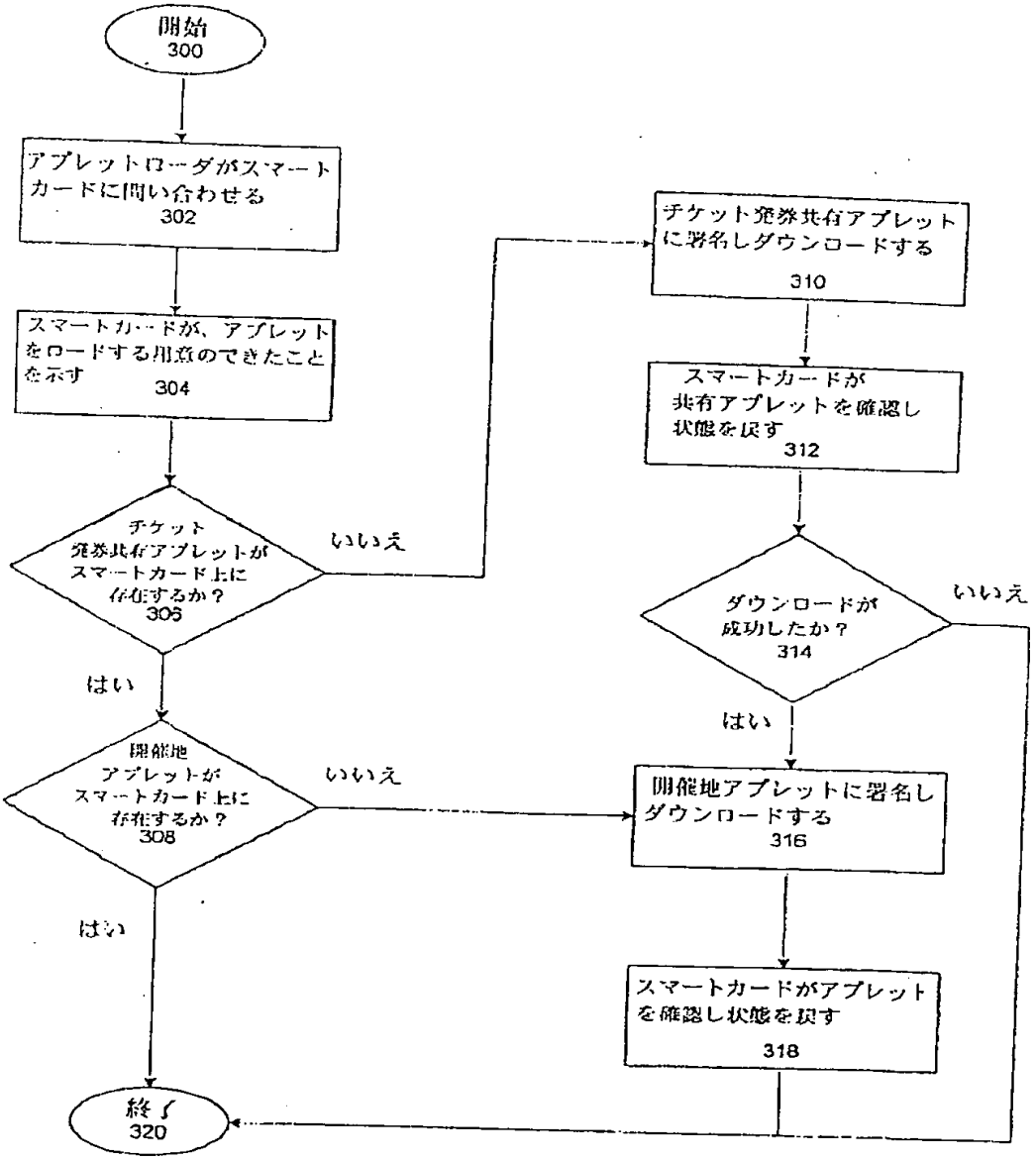
【図4】


開始
400
ユーザがチケットを選択しロードを開始する
402
チケットローダがスマートカードをチャレンジする
404
スマートカードがチャレンジに(開催地鍵を用いて)署名しそれを戻す
406
チケットローダが署名を確認する
408
チケット属性情報が生成および署名される
410
チケットがスマートカード上にダウンロードされる
412
開催地アプレットがチケット署名を確認する
414
終了
416

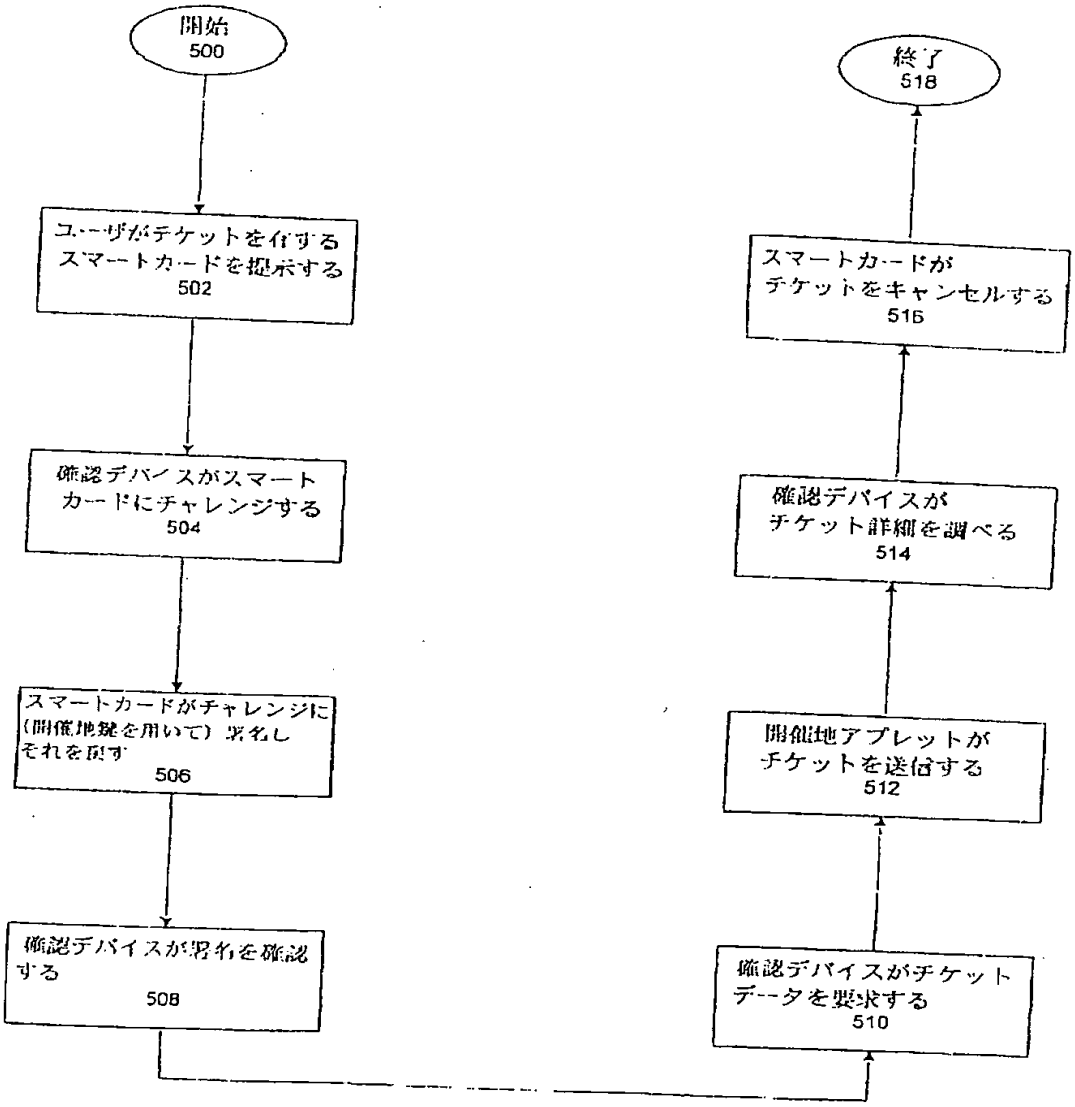
【図2】


共有アプレット
202
開催地ロータ鍵
202a
アプレットロータ鍵
200a
アプレット署名
202b
オペレーティングシステム(Java Virtual Machineを有する) 200
UNITED AIRLINES
チケットアプレット
220
開催地鍵
220a
アプレット署名
220b
開催地署名
220c
航空便007
SFOからPITへ
9/25/98
座席 4B
222
チケット署名
222a
SAN FRANCISCO GIANTS
チケットアプレット
210
開催地鍵
210a
アプレット署名
210b
開催地署名
210c
PITTSBURGH
PIRATES
9/22/98
座席 24A
212
チケット署名
212a
PITTSBURGH
PIRATES
9/23/98
座席 41D
214
チケット署名
214a
PITTSBURGH
PIRATES
9/24/98
座席 15C
216
チケット署名
216a

【図3】


開始
300
アプレットローダがスマートカードに問い合わせる
302
スマートカードが、アプレットをロードする用意のできたことを示す
304
チケット発券共有アプレットがスマートカード上に存在するか？
305
いいえ
はい
開催地アプレットがスマートカード上に存在するか？
308
いいえ
はい
チケット発券共有アプレットに署名しダウンロードする
310
スマートカードが共有アプレットを確認し状態を戻す
312
ダウンロードが成功したか？
314
いいえ
はい
開催地アプレットに署名しダウンロードする
316
スマートカードがアプレットを確認し状態を戻す
318
終了
320

【図5】



フロントページの続き

(72)発明者 セオドール チャールズ ゴールドスティン
アメリカ合衆国 カリフォルニア 94306, パロ アルト, ラパラ アベニュー 875

(72)発明者 ジョナサン ピー. ジエグラー
アメリカ合衆国 カリフォルニア 95014, クペルティノ, サンタ ルシア ロード 10611